PCT/CN2004/000997

证　　明

本证明之附件是向本局提交的下列专利申请副本

申　请　日：　2003.10.30

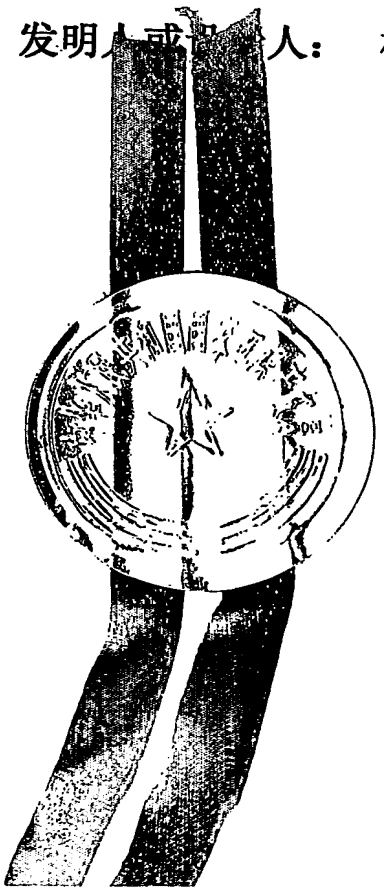
申　请　号：　2003101034007

申请类别：　发明

发明创造名称：　一种以太网二层交换设备绑定硬件地址和端口的方法

申　请　人：　华为技术有限公司

发明人或设计人：　杨磊



中华人民共和国
国家知识产权局局长　王景川

2004 年 10 月 21 日

权 利 要 求 书

1、一种以太网二层交换设备绑定硬件地址和端口的方法，至少包括如下步骤：

a. 在以太网二层交换设备检测到端口和终端设备的新建连接并接收到来自该终端设备的数据后，建立并保存该端口和该终端设备的硬件地址的固定对应关系，并根据所述固定对应关系转发数据；

b. 在以太网二层交换设备检测到端口和终端设备的连接断开后，删除所保存的所述固定对应关系。

2、根据权利要求 1 所述的以太网二层交换设备绑定硬件地址和端口的方法，其特征是，在步骤 a 中建立并保存所述固定关系之前进一步包括：在接收到来自该终端设备的数据之后判断是否已经建立了所述固定关系，如果是，直接转发数据，否则，执行步骤 a 中建立并保存该端口和该终端设备的硬件地址的固定对应关系的步骤。

3、根据权利要求 2 所述的以太网二层交换设备绑定硬件地址和端口的方法，其特征是，所述直接转发数据包括：判断数据中携带的硬件地址是否和所述固定对应关系中该端口对应的硬件地址一致，如果是，按照正常处理流程转发数据；否则丢弃该数据。

4、根据权利要求 3 所述的以太网二层交换设备绑定硬件地址和端口的方法，其特征是，在丢弃数据之后进一步包括：将判断结果记录在日志中并通知网络管理员。

5、根据权利要求 1 所述的以太网二层交换设备绑定硬件地址和端口的方法，其特征是，所述硬件地址是媒体访问控制（MAC）地址。

6、根据权利要求 1 所述的以太网二层交换设备绑定硬件地址和端口的方法，其特征是，所述检测终端设备和端口的新建连接以及检测终端设备和端口的连接断开是通过检测端口的物理信号进行的。

7、根据权利要求 1 所述的以太网二层交换设备绑定硬件地址和端口的方

法，其特征是，所述二层交换设备是二层交换机、三层交换机、防火墙设备或以太网桥。

8、根据权利要求 1 所述的以太网二层交换设备绑定硬件地址和端口的方法，其特征是，所述终端设备是个人计算机、服务器或网际协议（IP）电话机。

9、根据权利要求 1 所述的以太网二层交换设备绑定硬件地址和端口的方法，其特征是，所述固定关系保存在二层交换设备的硬件地址表中。

说　明　书

一种以太网二层交换设备绑定硬件地址和端口的方法

技术领域

本发明涉及网络安全领域，尤其涉及一种以太网二层交换设备绑定硬件地址和端口的方法。

背景技术

当前，网络病毒的破坏性越来越多样化，出现了许多新的破坏手段。对于网络可靠性的攻击就是这些新的破坏手段的一种。这种攻击不以盗取信息为目的，而是针对网络中的漏洞，对网络设备进行攻击，破坏网络的正常通讯，从而造成网络瘫痪，给用户带来更大的损失。对以太网的攻击是这种攻击的一种常见方式。

在以前的网络中，以太网多出现在内网之中，而传统的网络管理认为，内网是非常安全的，因此只对于内网的出口设置了网络安全防范策略，而在内网内部并未设置防范措施。同时，由于内网中客户的不同，导致网络管理部门无法实现对内网中的每个用户的网络使用进行监控，这样，随着计算机病毒不断出现新的破坏手段，以及很多容易被攻击的中低端网络产品得到了更多应用，从而使对以太网的攻击更加容易。另外，随着宽带的兴起和新型业务的普及，以太网越来越多地应用于相对于网络管理部门的外网中，以太网接入的宽带小区就是其中一例，在这种情况下，以太网更易受到攻击。

对于采用以太网实现通讯的用户来说，一旦以太网受到攻击，造成网络瘫痪，即使没有丢失任何有价值的资料，也会造成与网络瘫痪时间成正比的非常大的损失，而对于利用以太网进行工作业务的公司来说，这种损失往往比丢失资料更为严重。

在以太网中，主机的地址通过媒体访问控制（MAC）地址来标识。在

发送数据时，需要在数据报文中携带目的 MAC 地址信息和源 MAC 地址信息。以太网的二层交换设备，例如交换机，通过 MAC 地址信息来确定数据报文的转发端口。目前的交换机在转发数据报文时都是基于 MAC 学习机制的。如图 1 所示，例如个人计算机（PC）1 的 MAC 地址是 MAC1，PC2 的 MAC 地址是 MAC2。当交换机接收到 PC1 发出的数据报文时，记录该报文携带的 MAC 地址信息和接收到的端口信息，也就是建立 MAC1 和 Port1 的对应关系。与此相似，建立 MAC2 和 Port2 的对应关系。这样交换机可以建立所有的主机的 MAC 地址信息和相应端口信息之间的对应关系，并将其存储在 MAC 表中。在图 1 中，这个 MAC 表有两个表项，其中 MAC1 对应 Port1，MAC2 对应 Port2。当交换机接收到需要发送给 PC1 的数据报文时，首先根据 PC1 的 MAC 地址 MAC1 从 MAC 表中查找到相应的端口 Port1，然后将该数据报文通过该端口发送给 PC1。

在上述 MAC 地址的学习过程中，没有任何的认证机制，这样恶意用户可以据此对以太网中的单个用户或者整个以太网发起攻击。这种攻击可以通过 MAC 欺骗的方法来进行，也可以通过 MAC 轰炸的方法来进行。

图 2 示出了进行 MAC 欺骗的攻击过程示意图。如图 2 所示，如果 PC2 的用户是一个恶意用户并且希望攻击 PC1，那么 PC2 可以向交换机发送一个源 MAC 地址是 PC1 的 MAC 地址 MAC1 的数据报文，这时交换机会进行学习，从而建立 MAC1 和 Port2 的对应关系，也就是说，交换机中的 MAC 表中的 MAC1 和 Port1 的对应关系将在这次学习之后更改为 MAC1 和 Port2 的对应关系。这样，所有希望发送给 PC1 的数据报文都会发送到 Port2，从而发送给 PC2，导致 PC1 不能正常接收信息。如果恶意用户对以太网中的多台甚至所有的主机都采用同样的方法，那么整个以太网将濒于瘫痪。

除了上述 MAC 欺骗的方式之外，恶意用户也可以采用 MAC 轰炸的方法来攻击以太网。例如，恶意用户 PC2 可以不断地发出源 MAC 地址变化的数据报文，例如在第一个数据报文中 MAC 地址为 MAC1，而在第二个数据

报文中 MAC 地址换为 MAC3，在第三个数据报文中 MAC 地址又换为 MAC8。这样每接收到一个数据报文，交换机就需要更新 MAC 表，从而使交换机的 MAC 表始终处于一个不稳定的状态。如果这些源 MAC 地址信息中包含以太网中某个网络设备的真实地址，那么这个网络设备将不能进行正常的通讯。这种方式通常会被病毒所利用，通过被感染病毒的主机对整个以太网进行 MAC 轰炸，从而破坏整个以太网的正常运行。

为了避免上述情况对以太网的攻击，目前在交换机上普遍实行主机 MAC 地址和端口进行绑定。也就是说，在交换机上指定某个端口和某个 MAC 地址建立固定的对应关系，不再学习任何动态的 MAC 地址，这样 MAC 地址和端口的对应关系不会由于新接收的数据报文而改变，从而使 MAC 表成为一个固定表。这样可以有效地避免 MAC 欺骗和 MAC 轰炸等攻击现象。

但是，这种 MAC 地址和端口的固定绑定关系具有一个非常大的缺点。具体地说，这种绑定关系需要网络管理员根据固定的网络连接情况对交换机进行设置，而且一旦完成设置以后，这个网络就处于一种固定模式之下。一台新的计算机或者其它的合法以太网设备连接到网络中后不能进行通信，当计算机更换了一块以太网网卡后，由于 MAC 地址的改变，该计算机也不能进行通信，并且，当把计算机从一个地方移动到另一个地方，也可能由于连接端口的改变而无法通信。在这些情况下，也就是在整个以太网的任何网络设备出现了端口或 MAC 地址变化的情况下，网络管理员必须及时地修改交换机的配置，从而给整个网络维护带来了极大的不便，并且增加了网络维护的成本。

发明内容

有鉴于此，本发明的主要目的在于提供一种以太网二层交换设备绑定硬件地址和端口的方法，该方法可以在保证以太网网络安全的情况下，简化对硬件地址和端口之间的对应关系的配置，增加网络管理的方便性，降低网络维护成本。

为了实现上述目的，根据本发明的以太网二层交换设备绑定硬件地址和端口的方法包括如下步骤：

a. 在以太网二层交换设备检测到端口和终端设备的新建连接并接收到来自该终端设备的数据后，建立并保存该端口和该终端设备的硬件地址的固定对应关系，并根据固定对应关系转发数据；

b. 在以太网二层交换设备检测到端口和终端设备的连接断开后，删除所保存的固定对应关系。

在上述方法中，在步骤 a 中建立并保存固定关系之前可以进一步包括：在接收到来自该终端设备的数据之后判断是否已经建立了固定关系，如果是，直接转发数据，否则，执行步骤 a 中建立并保存该端口和该终端设备的硬件地址的固定对应关系的步骤。其中，直接转发数据包括：判断数据中携带的硬件地址是否和固定对应关系中该端口对应的硬件地址一致，如果是，按照正常处理流程转发数据；否则丢弃该数据。并且，在丢弃数据之后，可以进一步将判断结果记录在日志中并通知网络管理员。

在上述方法中，硬件地址可以是 MAC 地址。

在上述方法中，检测终端设备和端口的新建连接以及检测终端设备和端口的连接断开是通过检测端口的物理信号进行的。

在上述方法中，二层交换设备可以是二层交换机、三层交换机、防火墙设备或以太网桥。终端设备可以是个人计算机、服务器或网际协议（IP）电话机。

在上述方法中，固定关系保存在二层交换设备的硬件地址表中。

从本发明的技术方案可以看出，在终端设备连接到二层交换设备并且发送有数据时，二层交换设备学习该端口的硬件地址，从而建立终端设备的硬件地址和该端口的对应关系。而在终端设备断开和二层交换设备的连接后，二层交换设备会删除该端口所建立的对应关系，在该端口再次连接原始终端设备或者在该端口连接有新的终端设备时，二层交换设备再重新通过学习建立硬件地址和端口的对应关系。这样，相对于现有技术中建立固定的对应关

系表，对表中表项的修改需要由网络管理员手动完成而言，本发明会自动删除旧的对应关系和建立新的对应关系，从而给网络管理员带来了更大的方便，有效提高了网络维护的效率，降低了网络维护的成本。

另外，和硬件地址表可以不断更新的情况相比，本发明中一旦建立了硬件地址表，除非检测到终端设备和二层交换设备的连接断开，硬件地址表中该端口的对应关系都相对固定，不会接收一次数据就进行一次更改。因此，本发明可以有效地避免现有技术中 MAC 欺骗和 MAC 轰炸的现象，从而提高了网络的安全性和可靠性。

附图说明

图 1 为 IP 以太网中 MAC 学习机制的示意图。

图 2 为 IP 以太网中 MAC 欺骗的攻击过程示意图。

图 3 为本发明的总体处理流程图。

具体实施方式

下面结合附图和具体实施例对本发明进行详细说明。

在以太网中，所有的转发数据都是来源于用户层网络中的用户设备，这些用户设备包括 PC、服务器、IP 电话等以太网终端设备，而与这些用户设备相连接的则是接入层的交换机。对于以太网终端设备来说，它们都有各自的 MAC 地址，这个 MAC 地址一般是不会变化的，也就是说，交换机每个端口对应的 MAC 地址一般不会变化。只有在用户更换整个终端设备、更换 PC 中的网卡或者长距离地移动终端设备的情况下，交换机该端口对应的 MAC 地址才有可能变化。而在上述情况下，都需要中断终端设备和交换机的物理连接。在本发明中对交换机采用了 MAC 学习机制，并且通过检测物理信号来检测终端设备和交换机的物理连接是否中断，来决定是否要更新 MAC 表，从而可以使本发明既可以避免例如 MAC 欺骗和 MAC 轰炸等恶意用户对以太网的攻击，又可以避免固定 MAC 表造成的系统维护不便和维护

成本高的缺点。

图 3 示出了本发明的总体处理流程图。下面结合图 3 对本发明进行详细说明。

在一个以太网终端设备和交换机的端口建立连接后，在步骤 301 中，交换机接收来自终端设备的数据报文。

在步骤 302 中，交换机接收到该数据报文后，首先判断接收数据报文的端口是否已经基于 MAC 学习机制在 MAC 表中建立该终端设备的 MAC 地址和相应端口的对应关系，如果还没有针对该终端设备进行 MAC 地址学习，执行步骤 303，否则执行步骤 305。

在步骤 303 中，交换机的端口进行 MAC 地址学习，也就是在 MAC 表中建立该终端设备和该端口之间的对应关系。

在步骤 304 中，按照现有技术转发数据报文的处理正常转发该数据报文。

在步骤 305 中，判断数据报文中的源 MAC 地址是否和 MAC 表中该端口对应的 MAC 地址一致，如果一致，表明该数据报文是来自 MAC 表中该终端对应的 MAC 地址所对应的终端设备，执行步骤 304；如果不一致，表明该数据报文可能是恶意用户伪造 MAC 地址所发的数据报文，执行步骤 306，也就是丢弃该报文。在判断出 MAC 地址不一致并丢弃报文后，可以进一步将这种不一致的情况记录在日志中并通知网络管理员。

通过上述步骤即完成对一次数据报文的转发，然后在步骤 307 中，交换机判断连接该端口的终端设备是否和交换机断开连接。如果连接断开，在步骤 308 中，交换机在当前的 MAC 表中删除和该端口相关联的 MAC 表项，也就是删除当前的终端设备的 MAC 地址和端口的对应关系，当前处理结束。如果在该端口再次连接有终端设备，例如是另一个终端设备，是同一个终端设备但更换了网卡，或者依然是原来的终端设备并且网卡也没有更换，都重新开始本发明的处理流程，也就是重新建立该端口连接的终端设备的 MAC

地址和该端口之间的对应关系。如果连接没有断开，则重复执行步骤 301 及其后续步骤。

在本发明中，检测终端设备和端口是否建立有连接是通过检测端口的物理信号来进行的。具体地说，当终端设备和端口建立连接并且在终端设备上电启动后，交换机可以通过端口检测到一个高电平，表示终端设备上电启动。而当终端设备和端口断开连接，包括终端设备断电的情况，交换机可以通过端口检测到低电平，从而表示终端设备已经断开了交换机端口的连接，这时交换机就会删除 MAC 表中原有对应该端口的表项。

在本发明中，通过基于 MAC 学习机制来建立终端设备的 MAC 地址和交换机端口之间的对应关系，避免了 MAC 地址信息和端口固定绑定所带来的维护效率低和成本高的缺点，同时只要终端设备和端口没有断开连接，MAC 地址表中和该端口对应的表项就不会更改，这样在 PC 上运行伪造 MAC 地址的软件将不会影响交换机的 MAC 表，从而避免了 MAC 欺骗和 MAC 轰炸等现象。因此本发明通过终端设备和端口的动态绑定，既提高了网络的安全性和可靠性，又提高了网络的维护效率，降低了维护成本。

本领域技术人员可以理解，本发明中的交换机可以是二层交换机，也可以是三层交换机，并且本发明并不局限于交换机，而可以是任何二层交换设备，也就是任何支持以太网二层交换功能的设备，例如基于 MAC 学习的防火墙设备、以太网桥设备等。

因此，以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

说 明 书 附 图

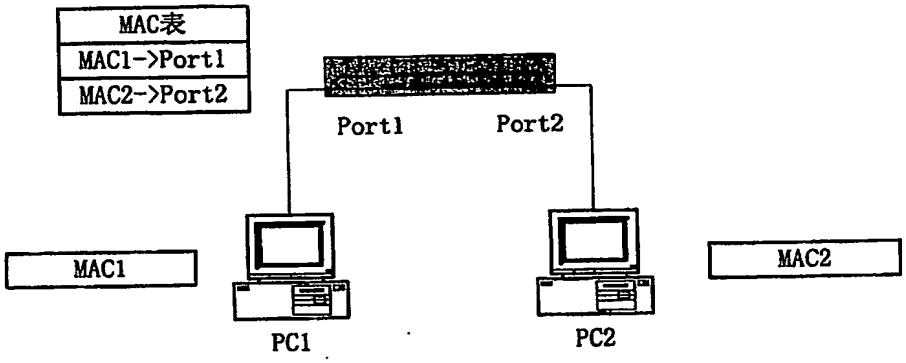

MAC表
MAC1->Port1
MAC2->Port2
Port1
Port2
MAC1
MAC2
PC1
PC2

图 1

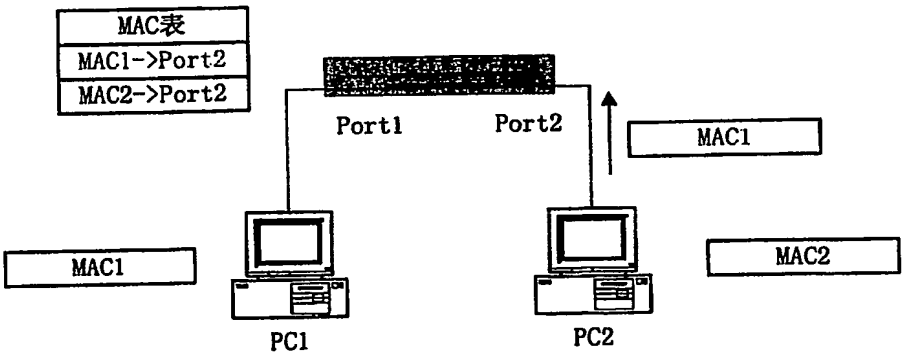

MAC表
MAC1->Port2
MAC2->Port2
Port1
Port2
MAC1
MAC1
MAC2
PC1
PC2

图 2

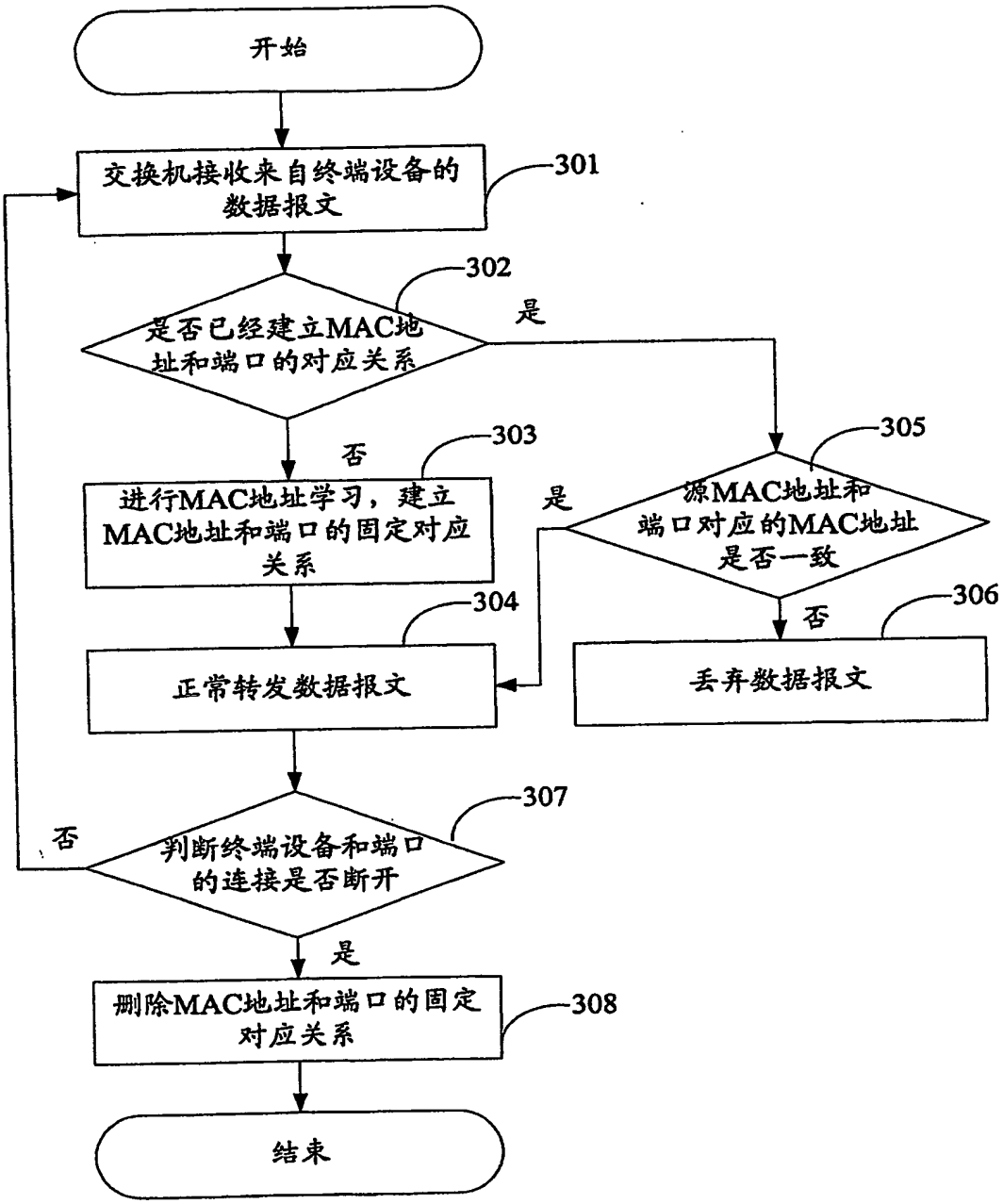

开始
交换机接收来自终端设备的数据报文
301
是否已经建立MAC地址和端口的对应关系
302
是
否
进行MAC地址学习，建立MAC地址和端口的固定对应关系
303
源MAC地址和端口对应的MAC地址是否一致
305
是
否
正常转发数据报文
304
丢弃数据报文
306
判断终端设备和端口的连接是否断开
307
否
是
删除MAC地址和端口的固定对应关系
308
结束

图 3